Gregory Blanc, Ph.D.

gregory.blanc@telecom-sudparis.eu @cloudgravity
https://cloudgravity.github.io/
https://fr.linkedin.com/in/gregory-blanc-970b381a
Office D101-01 RST department Télécom SudParis – 9 rue Charles Fourier F-91011 Evry

Professional Experience

Current Appointment

since 2015.06 — **Associate Professor in Networks and Security.** RST department, Télécom SudParis, **IMT** & UMR 5157 SAMOVAR, **CNRS**, Evry (FR).
conducts research in future networks (5G, IoT) and network virtualization security.
teaches web, application and network security.
coordinates the **Risk Analysis and Attack Detection** module in the Networks and Systems Security specialization course (SSR).
contributes to **CELTIC-PLUS SENDATE-TANDEM** project (2016.04 – 2019.03), **H2020 EUNITY** (2017.06 – 2019.05).
contributed to **H2020 SUPERCLOUD** project (2015.01 – 2018.02).

Past Experience

2012.09 – 2015.05 — **Research Engineer.** RST department, Télécom SudParis, **IMT** & UMR 5157 SAMOVAR, **CNRS**, Evry (FR). (formerly postdoctoral research associate until Sep 2014)
conducted research on threat data analysis and SDN-based resilience in the joint collaborative European-Japanese **FP7 NECOMA** project (2013.06 – 2016.03).
contributed to the European **ITEA2 ADAX** project (2013.01 – 2014.01).
conducted research in access control, supervised research interns and taught web security and assisted in teaching networking basics in the SSR specialization course.

2010.10 – 2012.03 — **Research Assistant.** Graduate School of Information Science, **Nara Institute of Science and Technology (NAIST)**, Ikoma (JP). (part-time position)
conducted research on client-side malicious code execution in the **Web 2.0 Security Management** project.
assisted in teaching networking basics to Master's students.

2010.03 – 2012.03 — **WG Leader.** Security in Web 2.0 Application (SWAN), **WIDE Project** (JP).
conducted R&D on Web application security and Web test platforms

2008.04 – 2008.12 — **Junior Consultant.** Security Solutions Integrations, **BT CyberNetworks**, Puteaux (FR). (formerly R&D intern until 2008.09)
surveyed Web Applications Firewalls (WAF) solutions.
integrated security solutions (WAF, IDS, VPN) at customer companies.

2007.02 – 2007.09 — **Research Intern. Solution Crew, Inc.** and Graduate School of Information Science, **NAIST**, Ikoma (JP).
conducted research on inferring malicious flows trajectories in the **InterTrack** project.

---

*Last updated: 5th March 2019

Education

2009.04 – 2012.03 — **Ph.D., NAIST, Japan** in Information Science.
Thesis title: *Reversing Malicious Intents in Web Scripts: from Automating Deobfuscation to Assigning Concepts.*
Defend on Dec. 22^{nd}, 2016 at Ikoma
Thesis committee:
Pr. Suguru Yamaguchi, NAIST (Thesis director)
Pr. Minoru Ito, NAIST (Reviewer)
Pr. Hiroyuki Seki, NAIST (Reviewer)
Pr. Masakatsu Nishigaki, Shizuoka University (Examiner)
Assoc. Pr. Youki Kadobayashi, NAIST (Thesis co-advisor)

2007.10 – 2008.09 — **Specialized Master, Ecole Supérieure d'Informatique Electronique Automatique (ESIEA), France** in Networks and Information Security.

2004.09 – 2007.09 — **Engineering diploma (M.Sc.), ESIEA, France** in ICT.

Skills

Coding	Python, Ruby, Javascript (AJAX), Java, C/C++, shell.
Academics	algorithmics, graph theory, programming languages (imperative, object oriented, formal, functional), compilers, operation systems, databases, formal logic, networks, information and systems security
Networking	TCP/IP, L2/L3, routing (BGP/OSPF), MPLS, SDN
Security	intrusion detection, vulnerability detection, web security, virtualization, data recovery, access control, incident response, alert correlation
Languages	French (native), English (TOEIC 2011: 990), Japanese (JLPT 2011: N2), Spanish

Professional Activities

Doctoral Defense Committees

Pierre-Edouard Fabre	defended his thesis *Using Network Resources to Mitigate Volumetric DDoS* on December 13th, 2018 at Télécom SudParis, Evry
Oualid Koucham	defended his thesis *Intrusion Detection for Industrial Control Systems* on November 12th, 2018 at Gipsa-Lab, Saint-Martin-d'Hères
Rishikesh Sahay	defended his thesis *Policy-Driven Autonomic Cyberdefense using Software Defined Networking* on November 14th, 2017 at Télécom SudParis, Evry
François-Xavier Aguessy	defended his thesis *Dynamic Risk Assessment and Remediation using Bayesian attack models* on September 22nd, 2016 at Télécom SudParis
Yosra Ben Mustapha	defended her thesis *Alert Correlation: Towards an Efficient Response Decision Support* on April 3Oth, 2015 at Télécom SudParis, Evry

Responsibilities and Memberships

RESSI	Steering committee member since 2017
Cybersecurity France-Japan	Network Security and Performance Measurement (WG 7) co-chair since 2017

Professional Activities (continued)

CNRS GDR Sécurité Informatique
- Networks and Infrastructure Security WG member since 2017

WIDE Project
- member #1491 since 2009, former SWAN WG leader (2009 – 2012)

Conference Program Committee and Reviewing

2019
- RESSI (PC chair), IWSEC (PC)

2018
- ISNCC (PC), IWSEC (PC), ICICS (PC), 5G-NS (PC)

2017
- ATC (PC), DIMVA, ESORICS, IWSEC (PC), RAID, XDOM0 (PC)

2016
- ATC (PC), ICETE, ISC2, IWSEC (PC)

2015
- ICSOC, NSS, SECRYPT

2014
- BADGERS (PC), AIDP (PC), WiSEC, CANS, C&ESAR, NSS, SECRYPT

2013
- NSS, SECRYPT

Journal Editing and Reviewing

Elsevier
- Computers & Security, Computer Communications, Computers and Electrical Engineering

IEEE
- Communications Magazine, Transactions on Information Forensics and Security, Transactions on Intelligent Transport Systems, Transactions on Network and Service Management

Springer
- Frontiers of Information Technology & Electronic Engineering, International Journal of Information Security, World Wide Web: Internet and Web Information Systems

Others
- MISC Magazine

Conference and Workshop Organization

2018
- DIMVA – organization co-chair
  ESSoS – organization co-chair
  ICICS – publication co-chair

2017
- RESSI – challenge organization

2016
- PDCAT – session chair
  RESSI – challenge scenarization
  RAID – local arrangement co-chair, publication co-chair

2015
- RAID – publication chair

2014
- ATC – workshop co-chair

2013
- ICT – session chair, *Young Ambassador*

Competition Participation

2010
- MWS Cup – Soukai Security IT-Keys
  technical ranking: 3^{rd} (analysis of malicious binaries and drive-by download attack traces).

Professional Activities (continued)

Awards and Grants

2017.10 – 2020.09 — **IMT** Futur & Ruptures Ph.D Excellence Grant *(for the thesis of M. Shahid)*

2011.04 – 2012.03 — **NEC C&C Foundation** Grant for Non-Japanese Researcher.

2009.01 – 2010.06 — **French Ministry of Foreign Affairs**, Lavoisier Japan Grant.

Research Activities

Research Interests

Cybersecurity — Intrusion Detection and Monitoring, Virtualization/Softwarization based Security, DDoS Mitigation, Access Control, Phishing Mitigation, Training

Data Science — Data Mining, Machine Learning, Deep Learning, Graph Representation

Applications — Network, Cloud, IoT, Web

Research Projects

H2020 CSA EUNITY — aims to encourage, facilitate and develop the dialogue between Europe and Japan on cybersecurity and privacy research and innovation trends and challenges, in order to foster and promote cybersecurity activities in both regions. *Main tasks included the management of the project, the organization of the workshops and the related questionnaires, the organization of small-scale, topic-specific seminars for Japanese representatives and the dissemination of EUNITY results.* `https://www.eunity-project.eu/`

CELTIC-PLUS SENDATE-TANDEM — addresses the challenge for a new network infrastructure with reference to high volatile data traffic of mobile linked up objects. A dynamic switching and a reliable transport of huge amounts of data as well as a handover of sensible, time critical application data without any interruptions must be provided between data centers with security guarantees. *Main tasks included the design of the TANDEM security architecture for 5G slicing, the collaborative development of a secure path computation and virtual network embedding.* `http://www.sendate.eu/sendate-tandem/`

Research Activities (continued)

H2020 SUPERCLOUD

- researches and develops new security and dependability infrastructure management paradigm. Our approach is on one hand, User-Centric for self-service clouds-of-clouds, i.e., customers can define their own protection requirements and avoid provider lock-ins. On the other hand we focus on Self-Managed services for self-protecting clouds-of-clouds which can reduce administration complexity through automation. *Main tasks included the development of an autonomous policy framework for SDN-based network threat mitigation, the integration of partners' products in a testbed.* `https://supercloud-project.eu/`

FP7 NECOMA

- addresses the aspect of data collection, with the goal to expand existing mechanisms and orient them towards threat data analysis. Second, it addresses threat data analysis not only from the perspective of understanding attackers and vulnerabilities, but also from the point of view of the target and victim. Third, it aims to develop and demonstrate new cyberdefense mechanisms that leverage threat analysis metrics for deployment and evaluation. The results are showcased in demonstrators. *Main tasks included the development of an SDN-based DDoS mitigation framework, a collection of SSL scans, the proposition of a cross-layer threat data analysis framework, a survey of existing PEP systems and the management of the project.* `http://www.necoma-project.eu/`

ITEA2 ADAX

- aims to study feasibility of solutions enabling to detect complex attacks against an information system working in its complex environment and to react smartly and quickly to those attacks with adapted countermeasures. *Main tasks included the development of a countermeasure selection technique based on a geometrical approach.* `http://adax.boun.edu.tr/`

Research Students Supervision

Ph.D

- **Elkin Aguas** (2018 -): *Automated Defense System for Cybersecurity*
  Fabien Charmet (2017 -): *Preservation of Security Properties during the Migration of Virtual Topologies in a SDN Environment*
  Mustafizur Shahid (2017 -): *Deep Learning Empowered Network Forensics in SDN-enabled IoT Network*
  François Boutigny (2016 -): *Security and Trust in SDN-based Multi-tenant Virtualized Networks*
  Rishikesh Sahay (2013 - 2017, now at Denmark Technical University): *Policy-driven Autonomic Cyberdefense using Software-Defined Networking*

Research Activities (continued)

Postdoc

- Houda Jmila (Mar 2018 -): *Designing Security-aware Slice Requests*
  Ion Popescu (Feb - Dec 2017): *Integrating Software-Defined Network and Network Function Virtualization*

Master

- **Baptiste Tabary** (Télécom SudParis, Apr - Sep 2019): *Applications of Machine Learning to IoT Network Security*
  Erwan Goareguer (Télécom SudParis, Jun - Sep 2018): *Resilience in SDN Networks*
  Mustafizur Shahid (Télécom SudParis, Apr - Sep 2017): *Leveraging Machine Learning to Predict the Security Level of C/C++ Programs Source Code*
  Aurélie Bonavent (CFSSI, Apr - Sep 2017): *Legitimate Traffic Generation in Security Tool Testing Environments*
  Julien Schoumacher (Télécom ParisTech, Jul 2017 - Jan 2018): *SDN Controller Security: ONOS*
  Nitish Reekoye (Télécom SudParis, Apr - Sep 2016): *Security of the Internet of Things: And In-Depth Analysis of the AllJoyn Framework*
  Grégory Van Blitz (CFSSI, Apr - Sep 2016): *Security Analysis of a SDN Implementation*
  Amaury Coulomban (INSA Lyon, Apr - Sep 2015): *Amplification DDoS Attacks Detection and Classification using Machine Learning Algorithms*
  Pernelle Mensah (Télécom SudParis, Apr - Sep 2015): *Visually Mitigating User's Excessive Trust in HTTPS Certificates*
  Vincent Danché (Télécom SudParis, Apr - Sep 2014): *Cross-Layer Threat Data Analysis*
  Guillaume Charton (ESIEA, Apr - Sep 2013): *Conflict Management in OrBAC Security Policies*

Hosted Interns

- **Shun Yonamine** (Ph.D at NAIST, Jan - Feb 2019): *Towards Disclosing Intentions in Linux-base IoT Malware*
  Jema David Ndibwile (Ph.D at NAIST, Jun - Jul 2018): *Smartphone User Phishing Prevention by Measuring the User's Consciousness through Embedded Camera*
  Sachit Malik (B.Tech at IIT Delhi, May - Jul 2016): *Study of New Web Attacks*
  Daishi Ito (Master at NAIST, Mar - Jun 2015): *SDN Controller Security*
  Hirotaka Fujiwara (Master at NAIST, Sep - Dec 2014): *Obfuscation Features based Drive-by Download Attack Detection*

Teaching Activities

Coordination

Courses

Projects Supervision

Research Publications

Journal Articles

1. Sahay, R., **Blanc**, **G.**, Zhang, Z., & Debar, H. (2017, September). ArOMA: an SDN based Autonomic DDoS Mitigation Framework. *Computers & Security*, *70*, 482–499. (ISI ranked, 1 pt). doi:10.1016/j.cose.2017.07.008

2. **Blanc**, **G.** & Kadobayashi, Y. (2011, November). A Step towards Static Script Malware Abstraction: Rewriting Obfuscated Script with Maude. *IEICE TRANSACTIONS on Information and Systems*, *94*(11), 2159–2166. (ISI ranked, 1 pt). doi:10.1587/transinf.E94.D.2159

Books and Proceedings

1. Giuffrida, C., Bardin, S., & **Blanc**, **G.** (Eds.). (2018, June). Detection of Intrusions and Malware, and Vulnerability Assessment, Saclay: Springer, *10885*. doi:10.1007/978-3-319-93411-2

2. Naccache, D., Xu, S., Qing, S., Samarati, P., **Blanc**, **G.**, Lu, R., … Meddahi, A. (Eds.). (2018, October). Information and Communications Security, Lille: Springer, *11149*. doi:10.1007/978-3-030-01950-1

3. Monrose, F., Dacier, M., **Blanc**, **G.**, & Garcia-Alfaro, J. (Eds.). (2016, September). Research in Attacks, Intrusions, and Defenses, Paris: Springer, *9854*. doi:10.1007/978-3-319-45719-2

4. Bos, H., Monrose, F., & **Blanc**, **G.** (Eds.). (2015, November). Research in Attacks, Intrusions, and Defenses, Kyoto: Springer, *9404*. doi:10.1007/978-3-319-26362-5

Ranked International Conference Papers

1. Boutigny, F., Betgé-Brezetz, S., Debar, H., **Blanc**, **G.**, Lavignotte, A., & Popescu, I. (2018, February). Multi-provider Secure Virtual Network Embedding. In *Proceedings of the 9th IFIP International Conference on New Technologies, Mobility & Security (NTMS)*. (ISI ranked, 0.5 pt). Paris: IEEE. doi:10.1109/NTMS.2018.8328706

2. Fabre, P., Viinikka, J., Debar, H., & **Blanc**, **G.** (2018, July). Network Visibility-aware Blacklist Generation. In *Proceedings of the 13th International Conference on Internet Monitoring and Protection (ICIMP)*. (ISI ranked, 0.5 pt). Barcelona: IARIA. doi:(Accepted)

3. Charmet, F., Waldinger, R., **Blanc**, **G.**, Kiennert, C., & Toumi, K. (2017, October). Preserving Confidentiality during the Migration of Virtual SDN Topologies: A Formal Approach. In *Proceedings of the 16th IEEE International Symposium on Network Computing and Applications (NCA)*. (rank A, 1 pt). Cambridge: IEEE. doi:10.1109/NCA.2017.8171392

4. Aguessy, F.-X., Bettan, O., **Blanc**, **G.**, Conan, V., & Debar, H. (2016, September). Hybrid Risk Assessment Model based on Bayesian Networks. In *Proceedings of the 11th International Workshop on Security (IWSEC)*. (rank B, 0.5 pt) (Best student paper award). Tokyo: Springer. doi:10.1007/978-3-319-44524-3_2

5. Fabre, P.-E., Viinikka, J., Debar, H., & **Blanc**, **G.** (2016, November). ML: DDoS Damage Control with MPLS. In *Proceedings of the 21st Nordic Conference on Secure IT Systems (NordSec)*. (rank C). Oulu: Springer. doi:10.1007/978-3-319-47560-8_7

6. Toumi, K., Idress, M. S., Charmet, F., Yaich, R., & **Blanc**, **G.** (2016, December). Usage Control Policy Enforcement in SDN-based Clouds: A Dynamic Availability Service Use Case. In *Proceedings of the 18th IEEE Conference on High Performance Computings and Communications (HPCC)*. (rank B, 0.5 pt). Sydney: IEEE. doi:10.1109/HPCC-SmartCity-DSS.2016.0087

7. Kheir, N., **Blanc**, **G.**, Debar, H., Garcia-Alfaro, J., & Yang, D. (2015, May). WebVisor: An Automatic Tool to Classify C&C Malware Connections via URL Clustering. In *Proceedings of the 30th International Conference on ICT Systems Security and Privacy Protection (IFIP SEC)*. (rank B, 0.5 pt). Hamburg: Springer. doi:10.1007/978-3-319-18467-8_17

8. Ben Mustapha, Y., Debar, H., & **Blanc**, **G.** (2014, September). Policy Enforcement Point Model. In *Proceedings of the 10th International Conference on Security and Privacy in Communication Networks (SecureComm)*. (rank B, 0.5 pt). Beijing: Springer. doi:10.1007/978-3-319-23829-6_20

9. Wazan, A. S., **Blanc**, **G.**, Debar, H., & Garcia-Alfaro, J. (2013, July). Attribute-Based Mining Process for the Organization-Based Access Control Model. In *Proceedings of the 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)* (pp. 421–430). (rank A, 1 pt). Melbourne: IEEE. doi:10.1109/TrustCom.2013.53

10. **Blanc**, **G.**, Ando, R., & Kadobayashi, Y. (2011, February). Term-Rewriting Deobfuscation for Static Client-Side Scripting Malware Detection. In *Proceedings of the 4th IFIP International Conference on New Technologies, Mobility and Security (NTMS)* (pp. 1–6). (ISI ranked, 0.5 pt). Paris: IEEE. doi:10.1109/NTMS.2011.5720649

11. Chaisamran, N., Okuda, T., **Blanc**, **G.**, & Yamaguchi, S. (2011, July). Trust-Based VoIP Spam Detection Based on Call Duration and Human Relationships. In *Proceedings of the IEEE/IPSJ 11th International Symposium on Applications and the Internet (SAINT)* (pp. 451–456). (rank C). Munich: IEEE. doi:10.1109/SAINT.2011.84

12. **Blanc**, **G.** & Kadobayashi, Y. (2010b, November). Towards Revealing JavaScript Program Intents Using Abstract Interpretation. In *Proceedings of the Sixth Asian Internet Engineering Conference (AINTEC)* (pp. 87–94). (ISI ranked, 0.5 pt). Bangkok: ACM. doi:10.1145/1930286.1930298

Other Conference and Workshop Papers

1. **Blanc**, **G.**, Kheir, N., Ayed, D., Lefebvre, V., Montes de Oca, E., & Bisson, P. (2018, August). Towards a 5G Security Architecture: Articulating Software-Defined Security and Security as a Service. In *Proceedings of the Workshop on 5G Networks Security (5G-NS), ARES Projects Symposium 2018, ARES 2018*. Hamburg. doi:10.1145/3230833.3233251

2. Shahid, M., **Blanc**, **G.**, Zhang, Z., & Debar, H. (2018, December). IoT Devices Recognition Through Network Traffic Analysis. In *2018 IEEE International Conference on Big Data (Big Data)*. Seattle. doi:10.1109/BigData.2018.8622243

3. Sahay, R., **Blanc**, **G.**, Zhang, Z., Toumi, K., & Debar, H. (2017, April). Adaptive Policy-driven Attack Mitigation in SDN. In *Proceedings of the 1st Workshop on Security and Dependability of Multi-Domain Infrastructures (XDOM0)*. Belgrade: ACM. doi:10.1145/3071064.3071068

4. Mensah, P., **Blanc**, **G.**, Okada, K., Miyamoto, D., & Kadobayashi, Y. (2015, November). ANJA: Anti-Phishing JS-based Visual Analysis, to Mitigate Users' Excessive Trust in

SSL/TLS. In *Proceedings of the 4th International Workshop on Building Analysis Datasets and Gathering Experience Returns for Security (BADGERS)*. Kyoto: IEEE. doi:10.1109/BADGERS.2015.019

5. Miyamoto, D., **Blanc**, **G.**, & Kadobayashi, Y. (2015, November). Eye Can Tell: On the Correlation between Eye Movement and Phishing Identification. In *Proceedings of the 2015 International Data Mining and Cybersecurity Workshop (DMC)*. Istanbul: Springer. doi:10.1007/978-3-319-26555-1_26

6. Sahay, R., **Blanc**, **G.**, Zhang, Z., & Debar, H. (2015, February). Towards Autonomic DDoS Mitigation using Software Defined Networking. In *Proceedings of the NDSS Workshop on Security of Emerging Networking Technologies (SENT)*. San Diego: Usenix. doi:10.14722/sent.2015.23004

7. Gonzalez Granadillo, G., Ponchel, C., **Blanc**, **G.**, & Debar, H. (2014, June). Combining Technical and Financial Impacts for Countermeasure Selection. In *Proceedings of the 2014 International Workshop on Advanced Intrusion Detection and Prevention (AIDP)* (pp. 1–14). Marrakech: EPTCS. doi:10.4204/EPTCS.165.1

8. Miyamoto, D., Iimura, T., **Blanc**, **G.**, Tazaki, H., & Kadobayashi, Y. (2014, September). EyeBit: Eye-Tracking Approach for Enforcing Phishing Prevention Habits. In *Proceedings of the 3rd International Workshop on Building Analysis Datasets and Gathering Experience Returns for Security (BADGERS)*. Wrocław: IEEE. doi:10.1109/BADGERS.2014.14

9. Petsas, T., Okada, K., Tazaki, H., **Blanc**, **G.**, & Pawliński, P. (2014, June). A Trusted Knowledge Management System for Multi-layer Threat Analysis. In *Proceedings of the 7th International Conference on Trust and Trustworthy Computing (TRUST)* (pp. 214–215). Heraklion: Springer. doi:10.1007/978-3-319-08593-7_18

10. Pukkawanna, S., Kadobayashi, Y., **Blanc**, **G.**, Garcia-Alfaro, J., & Debar, H. (2014, September). Classification of SSL Servers based on their SSL Handshake for Automated Security Assessment. In *Proceedings of the 3rd International Workshop on Building Analysis Datasets and Gathering Experience Returns for Security (BADGERS)*. Wrocław: IEEE. doi:10.1109/BADGERS.2014.10

11. **Blanc**, **G.**, Miyamoto, D., Akiyama, M., & Kadobayashi, Y. (2012, March). Characterizing Obfuscated JavaScript Using Abstract Syntax Trees: Experimenting with Malicious Scripts. In *Proceedings of the 26th International Conference on Advanced Information Networking and Applications Workshops (WAINA)* (pp. 344–351). Fukuoka: IEEE. doi:10.1109/WAINA.2012.140

12. Takahashi, T., **Blanc**, **G.**, Kadobayashi, Y., Fall, D., Hazeyama, H., & Matsuo, S. (2012, April). Enabling secure multitenancy in cloud computing: Challenges and approaches. In *Proceedings of the 2nd Baltic Congress on Future Internet Communications (BCFIC)* (pp. 72–79). Vilnius: IEEE. doi:10.1109/BCFIC.2012.6217983

13. Fall, D., **Blanc**, **G.**, Okuda, T., Kadobayashi, Y., & Yamaguchi, S. (2011, August). Toward Quantified Risk-Adaptive Access Control for Multi-tenant Cloud Computing. In *Proceedings of the 6th Joint Workshop on Information Security (JWIS, now AsiaJCIS)*. Kaohsiung.

14. **Blanc**, **G.** & Kadobayashi, Y. (2010a, August). Towards Real-time JavaScript Deobfuscation for Analysis Purposes. In *Proceedings of the 5th Joint Workshop on Information Security (JWIS, now AsiaJCIS)*. Guanghzhou.

15. **Blanc**, **G.** & Kadobayashi, Y. (2009, August). Towards Learning Intentions in Web 2.0. In *Proceedings of the 4th Joint Workshop on Information Security (JWIS, now AsiaJCIS)*. Kaohsiung.

16. Hazeyama, H., **Blanc**, **G.**, & Kadobayashi, Y. (2008, February). sFlow-based AS Border Traceback. In *Proceedings of the Asia Pacific Regional Internet Conference on Operational Technologies (APRICOT)*. Taipei.

17. **Blanc**, **G.**, Hazeyama, H., & Kadobayashi, Y. (2007, August). Flow Direction Inferring Using BGP Information Encapsulated in sFlow Packets. In *Proceedings of the 2nd Joint Workshop on Information Security (JWIS, now AsiaJCIS)*. Tokyo.

Domestic Conference and Technical Reports

1. Charmet, F. & **Blanc**, **G.** (2018, May). *Secure Migration of Virtual SDN Topologies* (No. RESSI2018:190670). Rendez-vous de la Recherche et de l'Enseignement de la Sécurité des Systèmes d'Information (RESSI). La Bresse.

2. Pham, C., **Blanc**, **G.**, & Debar, H. (2018, May). *On Automatic Network Environment Cloning for Facilitating Cybersecurity Training and Testing* (No. RESSI2018:190470). Rendez-vous de la Recherche et de l'Enseignement de la Sécurité des Systèmes d'Information (RESSI). La Bresse.

3. Fujiwara, H., **Blanc**, **G.**, Hazeyama, H., Iimura, T., & Kadobayashi, Y. (2015, March). *Implementation and Evaluation of Drive by Download Attack Detection using the Features of the Obfuscation* (No. ICSS2014-71). IEICE. in Japanese.

4. Fujiwara, H., **Blanc**, **G.**, Hazeyama, H., & Kadobayashi, Y. (2014, November). *A Study of Drive by Download Attack detection using the features of the obfuscation* (No. ICSS2014-60). IEICE. in Japanese.

5. **Blanc**, **G.**, Akiyama, M., Miyamoto, D., & Kadobayashi, Y. (2011, October). *Identifying Characteristic Syntactic Structures in Obfuscated Scripts by Subtree Matching* (No. CSS2011-080). IPSJ.

6. Jingu, M., **Blanc**, **G.**, Okuda, T., & Yamaguchi, S. (2011, October). *A Transition Graph to Trace the Vulnerabilities up to its Effects* (No. CSS2011-036). IPSJ. in Japanese.

7. Miyamoto, D., **Blanc**, **G.**, & Akiyama, M. (2011, October). *A consideration for categorizing Javascript files based on Abstract Syntax Tree Fingerprinting* (No. CSS2011-079). IPSJ. in Japanese.

8. Takahashi, T., **Blanc**, **G.**, Kadobayashi, Y., Fall, D., Hazeyama, H., & Matsuo, S. (2011, November). *Multitenant Cloud Computing: Security Challenges and Approaches* (No. ICSS2011-36). IEICE. in Japanese.

9. Chaisamran, N., **Blanc**, **G.**, Okada, K., Okuda, T., & Yamaguchi, S. (2010, November). *Basic Trust Calculation to Prevent Spam in VoIP Network based on Call Duration : Single Hop Consideration* (No. IA2010-51). IEICE. http://ci.nii.ac.jp/naid/110008145048/en/

10. Morihisa, K., Jingu, M., Kanda, S., **Blanc**, **G.**, & Kadobayashi, Y. (2010, October). *Towards Extracting and Visualizing Malware Distribution Operations Based on Network Traffic Logs*. IPSJ. in Japanese.

11. Wang, X., Okada, K., **Blanc**, **G.**, Okuda, T., & Yamaguchi, S. (2010, October). *A Sybil Node Detection Method for Chord*. IPSJ. in Japanese.

Theses

1. **Blanc**, **G.** (2012, March). *Reversing Malicious Intents in Web Scripts: from Automating Deobfuscation to Assigning Concepts* (Doctoral dissertation, Nara Institute of Science and Technology, Ikoma).

2. **Blanc**, **G.** (2007, September). *Studies on the Implementation of a Border Traceback System using xFlows* (Master's thesis, École Supérieure d'Informatique Électronique Automatique, Paris).

Invited Talks

1. Leveraging softwarization and virtualization to secure 5G slices. (2018, September). Seminar at CSIT, Queen's University Belfast. Belfast. https://blogs.qub.ac.uk/csitseminarseries/dr-gregory-blanc-19-september-2018/
2. Machine Learning Based Intrusion Detection System for IoT Network. (2018, July). Talk at DATAIA-JST International Symposium on Data Science and AI. Paris. http://dataia.eu/actualites/dataia-jst-international-symposium-data-science-and-ai
3. Secure network slices, paths and functions. (2018, April). Invited talk at NEPS Workshop on Cybersecurity. Lille. https://zonehua.github.io/cybersecurity-seminar/
4. The NECOMA Project: Nippon-European Cyberdefense-Oriented Multilayer Analysis. (2017, February). Poster at the European Project Space held during the3rd International Conference on Information Systems Security and Privacy (ICISSP). Porto. http://www.icissp.org/?y=2017
5. Analyse de Menaces sur les Objets Connectés: Le cas du Framework AllJoyn. (2016, December). Talk at 30th congress "De Nouvelles Architectures de Communications" (DNAC). Paris. http://dnac2016.dnac.org
6. Building SDN-based Security Services in a 5G World. (2016, December). Tutorial at 17th International Conference on Parallel and Distributed Computing, Applications and Technologies (PDCAT). Guangzhou. http://sdcs.sysu.edu.cn/space/pdcat2016/Tutorials.html
7. Cyberdefense-oriented Multilayer Threat Analysis: Experiences of an International Research Collaboration. (2016, June). Invited talk at TELECOM Lille Security Day – Security of Next Generation Networks. Lille. https://sites.google.com/site/zonehua/Cover/research-seminar
8. Etudes sur l'analyse de code malveillant en JavaScript. (2011, February). Invited talk at ESIEA. Paris.
9. Measurement Research to the Web Calamity's Rescue. (2010, April). Talk at 3rd CAIDA-WIDE-CASFI Joint Measurement Workshop. Osaka. http://www.caida.org/workshops/wide-casfi/1004/
10. Naviguer sur le Web 2.0 en toute sécurité: analyse de code JavaScript côté client. (2010, November). Poster at Journée Francophone de la Recherche. Tokyo.
11. Web 2.0 Security. (2010, May). Tutorial at Internet Summit of Africa, Web Workshop (jointly with AfNOG/AfriNIC/AfREN). Kigali. http://web.archive.org/web/20120728015812/http://africaasia.net:80/2010-5-Web.html

In preparation

1. **Blanc**, **G.**, Machnicki, D., Diaz-Rodriguez, R., Kozakiewicz, A., Kadobayashi, Y., Sahay, R., & Pawliński, P. (2019). *NECOMA: Nippon-European Cyberdefense-Oriented Multilayer Analysis*. submitted as a chapter to the book "European Project Space on Networks, Systems and Technologies" to be published by SCITEPRESS.

References

Available on Request